APPLICATION UNDER UNITED STATES PATENT LAWS

Invention: **USER PLANE LOCATION BASED SERVICE USING MESSAGE TUNNELING TO SUPPORT ROAMING**

Inventor(s):

Yinjun ZHU

Manelli Denison & Selter PLLC
2000 M Street, NW
7th Floor
Washington, DC 20036-3307
Attorneys
Telephone: (202) 261-1000

This is a:

[ ] Provisional Application

[X] Regular Utility Application

[ ] Continuing Application

[ ] PCT National Phase Application

[ ] Design Application

[ ] Reissue Application

[ ] Plant Application

SPECIFICATION

USER PLANE LOCATION BASED SERVICE USING MESSAGE TUNNELING TO SUPPORT ROAMING

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to wireless and long distance carriers, Internet Service Providers (ISPs), and information content delivery services/providers and long distance carriers. More particularly, it relates to location services for the wireless industry.

2. Background of Related Art

It is desired to accurately locate the physical position of a wireless device (e.g., a wireless telephone) within a wireless network. There are currently two different types of architecture developed to accomplish a location based service (LSB): Control Plane location based services, and more recently User Plane location based services.

Older location based services utilize what is now called Control Plane location based services. A Control Plane location based service utilizes a management system to automate and build processes and perform inventory management. A Control Plane location based service utilizes control or signaling messages to determine the location of a particular wireless device.

A key difference between these two technologies is that a Control Plane solution uses a control channel to communicate with the wireless device, while a User Plane solution uses the subscriber's traffic channel itself (e.g. IP bearer or SMS) to communicate with the wireless device. A Control Plane solution requires software updates to almost all the existing network components and wireless devices, while a User Plane solution is recognized as a more feasible solution for carriers to provide location-based services.

The concept known as User Plane location based service makes use of the user's bearer channel itself, e.g., IP bearer or SMS, to

establish the communications required for initiating a positioning procedure. User Plane location based services have been introduced as an alternative location service architecture as defined in standard organizations, e.g., 3GPP.

Thus, User Plane location based services utilize contents of the communications itself to locate the wireless device. User Plane location based services focus on the TCP/IP capability of a wireless device such as a mobile telephone to generally bypass the carrier infrastructure and instead use, e.g., the Internet. There are significant advantages to the deployment of User Plane location based services, including an easier and more streamlined architecture than that of a Control Plane location based service. In this way, costly upgrades are avoided, and quick and relatively inexpensive deployment is possible using otherwise conventional system components.

In User Plane location based services, the inventors have noted that there is an issue related to location service procedure when the target mobile is roaming and IP bearer is used (IP bearer is the default bearer for User Plane location service solutions). Roaming refers to the physical movement of a wireless device among the territories covered by different wireless carriers.

In particular, based on conventional User Plane location service architecture, the target wireless device or mobile to be located must communicate with the Positioning Server (a.k.a. GMLC in 3GPP, MPC in 3GPP2) that is serving the cell where the wireless device camps. In this procedure, a PDP Context is established between the wireless device and the GGSN in the wireless device's Home Public Land Mobile Network (H-PLMN). The PDP Context is a communication channel established for the target wireless device to access IP networks, including an H-LCS Manager (a.k.a. H-GMLC in 3GPP, or H-MPC in 3GPP2), a Visited-LCS Manager (a.k.a. Visited-GMLC in 3GPP, or Visited MPC in

3GPP2), and/or a Positioning Server (a.k.a. SMLC in 3GPP, or PDE in 3GPP2).

However, the inventors herein realize that for security reasons, the IP networks of different PLMNs are separated with protective IP firewalls. Furthermore, inside a PLMN, the IP network is usually configured as a private network using private IP addresses. The IP connectivity to the Internet goes through a gateway router that provides NAT function. Yet, in currently defined User Plane location based services, a target wireless device must communicate with the positioning server in the Visited-PLMN via the GGSN in Home-PLMN, using the positioning server's private IP address provided by the Visited-LCS Manager. However, in a roaming scenario, it is realized that it is currently not permitted for a wireless device to communicate directly with a proper positioning server because of the various firewalls.

While User Plane location based solutions have been developed and deployed in a number of networks, support is not complete, especially when a GPRS IP bearer is used as the bearer. This invention introduces a methodology to resolve a key issue related to a roaming scenario for User Plane location based service solutions.

In conventional 3GPP network architectures, when a mobile initiates a packet data service session, called a PDP Context, the location SGNS will establish a connection to the GGSN indicated by an Access Point Name (APN) provided by the mobile. The GGSN identified by the APN usually resides in the Home Public Land Mobile Network (H-PLMN) of the mobile. So, in the roaming scenario, an IP bearer is established between the MS and the GGSN in the Home PLMN. Therefore, all the IP traffic to/from the mobile is tunneled to the Home PLMN.

With a Release 6 architecture of the 3GPP standard, a Gateway Mobile Location Center (GMLC) is able to communicate with other GMLCs that reside in different PLMNs, using an Lr interface. Thus,

the Lr interface is allowed to go though the firewalls of PLMNs, attempting to provide adequate services in a roaming scenario.

In a typical Mobile Terminating (MT) location service in a roaming scenario, the mobile or wireless device must communicate with the local positioning server of a User Plane location based service (sometimes referred to as "SMLC" using 3GPP standards terminology), to exchange location information and request assistance and a positioning calculation depending upon the particular positioning method being used.

However, during the MT location service procedure of a conventional User Plane location based service, a wireless device will be provided with the IP address of the local positioning server. As the inventors have appreciated, usually this IP address is a private IP address. Thus, while in theory full roaming support seems to be enabled, the inventors herein have appreciated that in reality the wireless device is not always able to reach this IP host from a private network (H-PLMN) because it is protected by firewalls.

There is the need to provide roaming support for a real-world subscriber utilizing a User Plane location based service in an existing GPRS network architecture.

SUMMARY OF THE INVENTION

In accordance with the principles of the present invention, message tunneling mechanism enables User Plane location service seamlessly supporting location based service even when the target subscriber is roaming in different networks.

In one aspect of the invention, a method of providing a User Plan location based service to a roaming wireless device comprises establishing a roaming interface between a home LCS manager of a home wireless carrier network and a visited LCS manager of a currently visited wireless carrier network. IP connectivity is directed over the Internet with the capability of being transmitted through a firewall in the home wireless

carrier network and through a firewall in the visited wireless carrier network. A message tunneling mechanism is provided to provide an uninterrupted communication path between a location service system and a wireless device being located.

BRIEF DESCRIPTION OF THE DRAWINGS

Features and advantages of the present invention will become apparent to those skilled in the art from the following description with reference to the drawings, in which:

Fig. 1 shows an exemplary user plane location service architecture in accordance with an embodiment of the present invention.

Fig. 2 shows exemplary user plane location service signaling based on the user plane location service accordance shown in Fig. 1.

Fig. 3 shows exemplary enhanced user plane location service signaling using message-tunneling mechanism, based on the user plane location service accordance shown in Fig. 1.

Fig. 4 shows an exemplary message flow for message tunneling to support roaming in a User Plane location based service, in accordance with the principles of the present invention.

Fig. 5 shows an exemplary message flow for message tunneling to support roaming in a User Plane location based service, where Visited-LCS Manager and Visited-Positioning Server are integrated in one device, in accordance with the principles of the present invention.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

The present invention relates to the provision of an improved User Plane location based service (LBS) architecture and message flow, enabling seamless User Plane location based services even when a mobile or wireless device has roamed among different carrier networks.

The present invention overcomes constraints inherent in the current protocol for roaming support defined by the Secure User Plane Location Service specification.

The inventive solution enables a location system to automatically fall back to a message tunneling mechanism to ensure the security of a communication path between the location service system and the target wireless device, ensuring that the communication path is uninterrupted as the wireless device travels.

Fig. 1 shows an exemplary user plane location service architecture in accordance with an embodiment of the present invention.

In particular, as shown in Fig. 1, a roaming interface (Lr) is established between LCS Managers (a.k.a. GMLCs in 3GPP, or MPCs in 3GPP2), which can direct IP connectivity through firewalls via the Internet. The inventive solution implements a message tunneling mechanism to provide end-to-end protocol connectivity via a Home-LCS Manager and/or a Visited-LCS Manager.

An important concept introduced by the present invention is the use of a messaging level tunneling via GMLCs using the Lr interface. With this method, a wireless device can communicate with the local positioning server, crossing PLMNs, to complete the requested User Plane positioning procedure.

Fig. 2 shows exemplary existing user plane location service signaling based on the user plane location service accordance shown in Fig. 1.

In particular, as shown in Fig. 2, when roaming UE needs to communicate with V-Positioning Server that resides in Visited PLMN, based on the procedure defined in User Plane LCS, it cannot even establish a TCP connection with the V-Positioning Server, although they are physically in the same network. Therefore, current User Plane architecture cannot support roaming scenarios for the mobile networks

using private IP address assignments (which is very common in the industry due to the limited resource of IP addresses).

Fig. 3 shows exemplary enhanced user plane location service signaling using message-tunneling mechanism, based on the user plane location service accordance shown in Fig. 1.

In particular, Fig. 3 illustrates the concept of message tunneling for User Plane LCS service in roaming scenarios. In this case, UE sends a User Plane message, which should be sent to the V-Positioning Server, to the Home-LCS Manager instead. The Home-LCS Manager encapsulates the received message in a generic message and sends it to the V-LCS Manager. With existing 3GPP Release 6 architecture, a LCS Managers (a.k.a GMLC in 3GPP) is able to communicate with other LCS Managers (or GMLCs) that reside in different PLMNs, using Lr interface, i.e. Lr interface is allowed to go though the firewalls of PLMNs. The V-LCS Manager also uses message tunneling mechanism to pass the message from the UE to the V-Positioning Server, via local IP network connectivity.

Fig. 4 shows an exemplary message flow for message tunneling to support roaming in a User Plane location based service, in accordance with the principles of the present invention.

<u>Step **A**</u>

As shown in step **A** of Fig. 4, upon receiving a location request from a location service enabled application, the LCS Agent **302** may authenticate the application. If authentication is successful, the LCS Agent **302** issues an MLP Location request to the Requesting-LCS Manager **304**, with which LCS Agent is associated, for an immediate location fix.

<u>Step **B**</u>

The Requesting-LCS Manager **304** authenticates the LCS Agent **302**, and verifies that the LCS Agent **302** is authorized for the service it requests, based on the lcs-client-id received.

By examining the received msid of the target subscriber, the R-LCS Manager **304** can identify the relevant Home-LCS Manager **306** based, e.g., on roaming agreements, or using domain name service (DNS) lookup mechanism similar to IETF RFC 2916. The mechanisms used to identify the relevant Home-LCS Manager **306** are known to those of ordinary skill in the art.

The R-LCS Manager **304** then forwards the location request to the Home-LCS Manager **306** of the target subscriber, using an Lr interface.

<u>Step **C**</u>

Upon receipt of a location request, the Home-LCS Manager **306** applies subscriber Privacy against lcs-client-id, requestor-id, qos, etc. that are received in the request. This use case assumes privacy check success. If the LCS Manager **304** did not authorize the application, step **N** will be returned with the applicable MLP return code.

The H-LCS Manager **306** then initiates the location processing with the user equipment (UE) **312** using a suitable LCS INIT message, e.g., a wireless application protocol (WAP) PUSH, or a short messaging system (SMS) Trigger, and starts a timer T1.

The H-LCS Manager **306** can optionally provide UE coarse position information to the UE at this time if the H-LCS Manager **306** has knowledge of the coarse position.

If the result of the privacy check in Step **B** indicates that notification or verification to the target subscriber is needed, the H-LCS Manager **306** may also include a notification element in the LCS INIT message.

Step **D**

If Notification/Verification is required, UE popup text may be used to notify the subscriber who is requesting his/her location info, e.g., lcs-client-id, requestor-id, request-type, etc. Optionally, the subscriber may be allowed to either grant the location request or deny the location request.

If the target subscriber grants the location request, the UE **312** starts the positioning procedure by retrieving the current serving cell information, TA, NMR, and mobile device capabilities. The UE **312** then initiates a location session with the H-LCS Manager **306** using Start Location Request (SLREQ), with cell info and optional AD, TA and NMR if the UE needs to obtain assistance data, and/or TA and NMR are available. Optionally, the UE **312** also indicates whether the target subscriber has been granted access when verification is required in the LCS INIT message.

If the target subscriber denies the location request, the UE **312** initiates a location response to the H-LCS Manager **306** including indication of the denial.

When the H-LCS Manager **306** receives the SLREQ message from the target subscriber for the pending transaction, it stops the timer T1.

Step **E**

If the target subscriber has denied the location request in Step **D**, Step **L** will be returned with the applicable MLP return code. In this case, Steps **E** to **K** are skipped. Otherwise, with the cell information from the target UE **312** (or via another mechanism), the H-LCS Manager **306** can determine that the target UE **312** is roaming. Based on a relevant roaming agreement, or using a DNS lookup mechanism similar to IETF RFC 2916, the H-LCS Manager **306** can identify the Visited-LCS Manager **308**, and initiates an Lr request to the Visited-LCS Manager **308,** with an

indicator that message tunneling mechanism will be used for this transition.

Step **F**

When receiving the Lr request, the Visited-LCS Manager **308** initiates a Position Request (PREQ), with optional cellinfo, NMR, device cap, etc., to the Positioning Server **310** that serves the area where target UE **312** currently is located.

Step **G**

The Positioning Server **310** sends a Position Response (PRESP) back to the V-LCS Manager **308**, and confirms that the Positioning Server **310** is ready to process the location request identified by sessionid.

Step **H**

Upon receipt of the Position Response message, the V-LCS Manager **308** sends an Lr Response message to the H-LCS Manager **306**. The Lr Response message may include, e.g., the IP address (URL) of the Positioning Server **310**.

Step **I**

Upon receiving the confirmation of the PRESP message from the serving Positioning Server **310**, the H-LCS Manager **306** sends a Start Location Response (SLRESP) message with the address of the H-LCS Manager **306** instead of V-Positioning Server for non-roaming scenario, if direct communication between the serving Positioning Server **310** and the target UE **312** is required, and an optional posmode to the target UE **312**.

Note, importantly, that the provided address of the serving Positioning Server **310** may be a private IP address in the roaming scenario.

Step **J**

Upon detection of roaming for the relevant UE 312, the target UE **312** initiates position determination, e.g., Position Determination Initiation (PDINIT), and sessionid, to the H-LCS Manager **306**. The PDINIT message optionally contains additional information, e.g., cell id, ad, and/or IS-801 PDU.

Step **K**

When receiving the message, the H-LCS Manager **306** forwards the PDINIT message inside a Position Data message corresponding to the sessionid to the V-LCS Manager **308** via the relevant Lr connection.

Step **L**

The V-LCS Manager **308** forwards the received Position Data message to the serving Positioning Server **310**.

Step **M**

The Positioning Server **310** and the target UE **312** start a precise positioning procedure by exchanging Position Determination Messaging (PDMESS) messages encapsulated by Position Data as illustrated in Steps **J**, **K** and **L**, via the H-LCS Manager **306** and the V-LCS Manager **308**.

Importantly, the positioning procedure itself may be, e.g., an RRLP, IS-801, or RRC based transaction. However, the positioning procedure (e.g., RRLP, IS-801 or RRC) protocol is tunneled in PDMESS

messages, which are tunneled by generic Position Data messages that are transported between H-LCS Manager and V-LCS Manager.

Step **N**

The Positioning Server **310** may send a Position Report (PRPT) to the R/H/V-LCS Managers **304**, **306**, **308** with the determined location information from the target UE **312**.

Steps **O, P**

Upon receiving the required position estimates from the Position Report (PRPT), the Visited-LCS Manager **308** forwards the location estimate to the Home-LCS Manager **306** using an Lr response message.

Step **Q**

The Home-LCS Manager **306** forwards the location estimate to the Requesting-LCS Manager **304** if the location estimate is allowed by the privacy settings of the target subscriber.

Step **R**

Finally, the Requesting-:LCS Manager **304** sends an MLP SLIA message with location estimates back to the LCS Agent **302**.

Fig. 5 shows an exemplary message flow for message tunneling to support roaming in a User Plane location based service, where Visited-LCS Manager and Visited-Positioning Server are integrated in one device, in accordance with the principles of the present invention.

Step **A**

As shown in step **A** of Fig. 4, upon receiving a location request from a location service enabled application, the LCS Agent **302** may authenticate the application. If authentication is successful, the LCS

Agent **302** issues an MLP Location request to the Requesting-LCS Manager **304**, with which LCS Agent is associated, for an immediate location fix.

<u>Step **B**</u>

The Requesting-LCS Manager **304** authenticates the LCS Agent **302**, and verifies that the LCS Agent **302** is authorized for the service it requests, based on the lcs-client-id received.

By examining the received msid of the target subscriber, the R-LCS Manager **304** can identify the relevant Home-LCS Manager **306** based, e.g., on roaming agreements, or using domain name service (DNS) lookup mechanism similar to IETF RFC 2916. The mechanisms used to identify the relevant Home-LCS Manager **306** are known to those of ordinary skill in the art.

The R-LCS Manager **304** then forwards the location request to the Home-LCS Manager **306** of the target subscriber, using an Lr interface.

<u>Step **C**</u>

Upon receipt of a location request, the Home-LCS Manager **306** applies subscriber Privacy against lcs-client-id, requestor-id, qos, etc. that are received in the request. This use case assumes privacy check success. If the LCS Manager **304** did not authorize the application, step **N** will be returned with the applicable MLP return code.

The H-LCS Manager **306** then initiates the location processing with the user equipment (UE) **312** using a suitable LCS INIT message, e.g., a wireless application protocol (WAP) PUSH, or a short messaging system (SMS) Trigger, and starts a timer T1.

The H-LCS Manager **306** can optionally provide UE coarse position information to the UE at this time if the H-LCS Manager **306** has knowledge of the coarse position.

If the result of the privacy check in Step **B** indicates that notification or verification to the target subscriber is needed, the H-LCS Manager **306** may also include a notification element in the LCS INIT message.

Step **D**

If Notification/Verification is required, UE popup text may be used to notify the subscriber who is requesting his/her location info, e.g., lcs-client-id, requestor-id, request-type, etc. Optionally, the subscriber may be allowed to either grant the location request or deny the location request.

If the target subscriber grants the location request, the UE **312** starts the positioning procedure by retrieving the current serving cell information, TA, NMR, and mobile device capabilities. The UE **312** then initiates a location session with the H-LCS Manager **306** using Start Location Request (SLREQ), with cell info and optional AD, TA and NMR if the UE needs to obtain assistance data, and/or TA and NMR are available. Optionally, the UE **312** also indicates whether the target subscriber has been granted access when verification is required in the LCS INIT message.

If the target subscriber denies the location request, the UE **312** initiates a location response to the H-LCS Manager **306** including indication of the denial.

When the H-LCS Manager **306** receives the SLREQ message from the target subscriber for the pending transaction, it stops the timer T1.

Step **E**

If the target subscriber has denied the location request in Step **D**, Step **L** will be returned with the applicable MLP return code. In this case, Steps **E** to **K** are skipped. Otherwise, with the cell information

from the target UE **312** (or via another mechanism), the H-LCS Manager **306** can determine that the target UE **312** is roaming. Based on a relevant roaming agreement, or using a DNS lookup mechanism similar to IETF RFC 2916, the H-LCS Manager **306** can identify the Visited-LCS Manager **308**, and initiates an Lr request to the Visited-LCS Manager **308,** with an indicator that message tunneling mechanism will be used for this transition.

<u>Step **F**</u>

The Positioning Server **310** and the target UE **312** start a precise positioning procedure by exchanging Position Determination Messaging (PDMESS) messages encapsulated by Position Data messages, via the H-LCS Manager **306** and the V-LCS Manager **308**.

Importantly, the positioning procedure itself may be, e.g., an RRLP, IS-801, or RRC based transaction. However, the positioning procedure (e.g., RRLP, IS-801 or RRC) protocol is tunneled in PDMESS messages, which are tunneled by generic Position Data messages that are transported between H-LCS Manager and V-LCS Manager.

<u>Steps **G**</u>

Upon receiving the required position estimates in Step **F**, the Visited-LCS Manager **308** forwards the location estimate to the Home-LCS Manager **306** using an Lr response message.

<u>Step **H**</u>

The Home-LCS Manager **306** forwards the location estimate to the Requesting-LCS Manager **304** if the location estimate is allowed by the privacy settings of the target subscriber.

<u>Step **I**</u>

Finally, the Requesting-:LCS Manager **304** sends an MLP SLIA message with location estimates back to the LCS Agent **302**.

While the invention has been described with reference to the exemplary embodiments thereof, those skilled in the art will be able to make various modifications to the described embodiments of the invention without departing from the true spirit and scope of the invention.